How an Israeli Spy-Linked Tech Firm Gained Access to the US Gov't's Most Classified Networks

Through its main investors, SoftBank and Lockheed Martin, Cybereason not only has ties to the Trump administration but has its software running on some of the U.S. government's most classified and secretive networks.

BY **WHITNEY WEBB** JANUARY 15, 2020 15 MINUTE READ

This article was originally published on MintPress News

If the networks of the U.S. military, the U.S. intelligence community and a slew of other U.S. federal agencies were running the software of a company with deep ties, not only to foreign companies with a history of espionage against the U.S. but also foreign military intelligence, it would — at the very least — garner substantial media attention. Yet, no media reports to date have noted that such a scenario exists on a massive scale and that the company making such software recently simulated the cancellation of the 2020 election and the declaration of martial law in the United States.

Earlier this month, *MintPress News* reported on the simulations for the U.S. 2020 election organized by the company Cybereason, a firm led by former members of Israel's military intelligence Unit 8200 and advised by former top and current officials in both Israeli military intelligence and the CIA. Those simulations, attended by federal officials from the FBI, DHS and the U.S. Secret Service, ended in

disaster, with the elections ultimately canceled and martial law declared due to the chaos created by a group of hackers led by Cybereason employees.

The first installment of this three part series delved deeply into Cybereason's ties to the intelligence community of Israel and also other agencies, including the CIA, as well as the fact that Cybereason stood to gain little financially from the simulations given that their software could not have prevented the attacks waged against the U.S.' electoral infrastructure in the exercise.

Also noted was the fact that Cybereason software could be potentially used as a backdoor by unauthorized actors, a possibility strengthened by the fact that the company's co-founders all previously worked for firms that have a history of placing backdoors into U.S. telecommunications and electronic infrastructure as well as aggressive espionage targeting U.S. federal agencies.

The latter issue is crucial in the context of this installment of this exclusive *MintPress* series, as Cybereason's main investors turned partners have integrated Cybereason's software into their product offerings. This means that the clients of these Cybereason partner companies, the U.S. intelligence community and military among them, are now part of Cybereason's network of more than 6 million endpoints that this private company constantly monitors using a combination of staff comprised largely of former intelligence operatives and an AI algorithm first developed by Israeli military intelligence.

Cybereason, thus far, has disclosed the following groups as lead investors in the company: Charles River Ventures (CRV), Spark Capital, Lockheed Martin and SoftBank. Charles River Ventures (CRV) was among the first to invest in Cybereason and has been frequently investing in other Israeli tech start-upsthat were founded by former members of the elite Israeli military intelligence Unit 8200 over the last few years. Spark Capital, based in California, appears to have followed CRV's interest in Cybereason since the venture capitalist who co-founded Spark and led its investment in Cybereason is a former CRV partnerwho still has close ties to the firm.

While CRV and Spark Capital seem like just the type of investors a company like Cybereason would attract given their clear interest in similar tech start-ups coming out of Israel's cyber sector, Cybereason's other lead investors — Lockheed Martin and SoftBank — deserve much more attention and scrutiny.

Cybereason widely used by US Government, thanks to Lockheed

"A match made in heaven," trumpeted *Forbes* at the news of the Lockheed Martin-Cybereason partnership, first forged in 2015. The partnership involved not only Lockheed Martin becoming a major investor in the cybersecurity company but also in Lockheed Martin becoming the largest conduit providing Cybereason's software to U.S. federal and military agencies.

Indeed, as *Forbes* noted at the time, not only did Lockheed invest in the company, it decided to integrate Cybereason's software completely into its product portfolio, resulting in a "model of both using Cybereason internally, and selling it to both public and private customers."

Cybereason CEO and former offensive hacker for Israeli military intelligence — Lior Div — said the following of the partnership:

Lockheed Martin invested in Cybereason's protection system after they compared our solution against a dozen others from the top industry players. The US firm was so impressed with the results they got from Cybereason that they began offering it to their own customers – among them most of the top Fortune 100 companies, and the US federal government. Cybereason is now the security system recommended by LM to its customers for protection from a wide (sic) malware and hack attacks."

Rich Mahler, then-director of Commercial Cyber Services at Lockheed Martin,told *Defense Daily* that the company's decision to invest in Cybereason, internally use its software, and include the technology as part of Lockheed Martin's cyber solutions portfolio were all "independent business decisions but were all coordinated and timed with the transaction."

How independent each of those decisions actually was is unclear, especially given the timing of Lockheed Martin's investment in Cybereason, whose close and troubling ties to Israeli intelligence as well as the CIA were noted in the previous installment of this investigative series. Indeed, about a year prior to their investment in the Israeli military intelligence-linked Cybereason, Lockheed Martin opened an office in Beersheba, Israel, where the IDF has its "cyberhub". The office is focused not on the sales of armaments, but instead on technology.

Marilyn Hewson, Lockheed Martin's CEO, said the following during her speechthat inaugurated the company's Beersheba office:

The consolidation of IDF Technical Units to new bases in the Negev Desert region is an important transformation of Israel's information technology capability…We understand the challenges of this move. Which is why we are investing in the facilities and people that will ensure we are prepared to support for these critical projects. By locating our new office in the capital of the Negev we are well positioned to work closely with our Israeli partners and stand ready to: accelerate project execution, reduce program risk and share our technical expertise by training and developing in-country talent."

Beersheba not only houses the IDF's technology campus, but also the Israel National Cyber Directorate, which reports directly to Israel's Prime Minister, as well as a high-tech corporate park that mostly houses tech companies with ties to Israel's military intelligence apparatus. The area has been cited in several media reports as a visible indicator of the public-private merger between Israeli technology companies, many of them started by Unit 8200 alumni, and the Israeli government and its intelligence services. Lockheed Martin quickly became a key fixture in the Beersheba-based cyberhub.

Not long before Lockheed began exploring the possibility of opening an office in Beersheba, the company was hacked by individuals who used tokens tied to the company, RSA Security, whose founders have ties to Israel's defense establishment and which is now owned by Dell, a company also deeply tied to the Israeli government and tech sector. The hack, perpetrated by still unknown actors, may have sparked Lockheed's subsequent interest in Israel's cybersecurity sector.

Soon after opening its Beersheba office, Lockheed Martin created its Israel subsidiary, Lockheed Martin Israel. Unlike many of the company's other subsidiaries, this one is focused exclusively on "cybersecurity, enterprise information technology, data centers, mobile, analytics and cloud" as opposed to the manufacture and design of armaments.

Haden Land, then-vice president of research and technology for Lockheed Martin, told *the Wall Street Journal* that the creation of the subsidiary was largely aimed at securing contracts with the IDF and that the company's Israel subsidiary would soon be seeking partnership and investments in pursuit of that end. Land oversaw the local roll-out of the company's Israel subsidiary while concurrently meeting with Israeli government officials. According to the *Journal*, Land "oversees all of Lockheed Martin's information-systems businesses, including defense and civilian commercial units" for the United States and elsewhere.

Just a few months later, Lockheed Martin partnered and invested in Cybereason, suggesting that Lockheed's decision to do so was aimed at securing closer ties with the IDF. This further suggests that Cybereason still maintains close ties to Israeli military intelligence, a point expounded upon in great detail in the previous installment of this series.

Thus, it appears that not only does Lockheed Martin use Cybereason's software on its own devices and on those it manages for its private and public sector clients, but it also decided to use the company's software in this way out of a desire to more closely collaborate with the Israeli military in matters related to technology and cybersecurity.

The cozy ties between Lockheed Martin, one of the U.S. government's largest private contractors, and the IDF set off alarm bells, then and now, for those concerned with U.S. national security. Such concern makes it important to look at the extent of Cybereason's use by federal and military agencies in the United States through their contracting of Lockheed Martin's Information Technology (IT) division. This is especially important considering Israeli military intelligence's history of using espionage, blackmail and private tech companies against the U.S. government, as detailed here.

While the exact number of U.S. federal and military agencies using Cybereason's software is unknown, it is widespread, with Lockheed Martin's IT division as the conduit. Indeed, Lockheed Martin was the number one IT solutions provider to the U.S. federal government up until its IT division was spun off and merged with Leidos Holdings. As a consequence, Leidos is now the largest IT provider to the U.S. government and is also directly partnered with Cybereason in the same way Lockheed Martin was. Even after its IT division was spun off, Lockheed Martin continues to use Cybereason's software in its cybersecurity work for the Pentagon and still maintains a stake in the company.

The Leidos-Lockheed Martin IT hybrid provides a litany of services to the U.S. military and U.S. intelligence. As investigative journalist Tim Shorrock noted for *The Nation*, the company does "everything from analyzing signals for the NSA to tracking down suspected enemy fighters for US Special Forces in the Middle East and Africa" and, following its merger with Lockheed and consequential partnership with Cybereason, became "the largest of five corporations that together employ nearly 80 percent of the private-sector employees contracted to work for US spy and surveillance agencies." Shorrock also notes that these private-sector contractors now dominate the mammoth U.S. surveillance apparatus, many of them working for Leidos and — by extension — using Cybereason's software.

Leidos' exclusive use of Cybereason software for cybersecurity is also relevant for the U.S. military since Leidos runs a number of sensitive systems for the Pentagon, including its recently inked contract to manage the entire military telecommunications infrastructure for Defense Information Systems Agency (DISA). In addition to maintaining the military telecom network, Cybereason is also directly partnered with World Wide Technologies (WWT) as of this past October. WWT manages cybersecurity for the U.S. Army, maintains DISA's firewalls and data storage as well as the U.S. Air Force's biometric identification system. WWT also manages contracts for NASA, itself a frequent

target of Israeli government espionage, and the U.S. Navy. WWT's partnership is similar to the Lockheed/Leidos partnership in that Cybereason's software is now completely integrated into its portfolio, giving the company full access to the devices on all of these highly classified networks.

Many of these new partnerships with Cybereason, including its partnership with WWT, followed claims made by members of Israel's Unit 8200 in 2017 that the popular antivirus software of Kaspersky Labs contained a backdoor for Russian intelligence, thereby compromising U.S. systems. The *Wall Street Journal* was the first to report on the alleged backdoor but did not mention the involvement of Unit 8200 in identifying it, a fact revealed by the *New York Times* a week later.

Notably, none of the evidence Unit 8200 used to blame Kaspersky has been made public and Kaspersky noted that it was actually Israeli hackers that had been discovered planting backdoors into its platform prior to the accusation levied against Kaspersky by Unit 8200. As the *New York Times* noted:

Investigators later discovered that the Israeli hackers had implanted multiple back doors into Kaspersky's systems, employing sophisticated tools to steal passwords, take screenshots, and vacuum up emails and documents."

Unit 8200's claims ultimately led the U.S. government to abandon Kaspersky's products entirely in 2018, allowing companies like Cybereason (with its own close ties to Unit 8200) to fill the void. Indeed, the very agencies that banned Kaspersky now use cybersecurity software that employs Cybereason's EDR system. No flags have been raised about Cybereason's own collaboration with the very foreign intelligence service that first pointed the finger at Kaspersky and that previously sold software with backdoors to sensitive U.S. facilities.

SoftBank, Cybereason and the Vision Fund

While its entry into the U.S. market and U.S. government networks is substantial, Cybereason's software is also run throughout the world on a massive scale through partnerships that have seen it enter into Latin American and European markets in major ways in just the last few months. It has also seen its software become prominent in Asia following a partnership with the company Trustwave. Much of this rapid expansion followed a major injection of cash courtesy of one of the company's biggest clients and now its largest investor, Japan's SoftBank.

SoftBank first invested in Cybereason in 2015, the same year Lockheed Martin initially invested and partnered with the firm. It was also the year that SoftBank announced its intention to invest in Israeli tech start-ups. SoftBank first injected $50 million into Cybereason, followed by an additional $100 million in 2017 and $200 million last August. SoftBank's investments account for most of the moneyraised by the company since it was founded in 2012 ($350 million out of $400 million total).

Prior to investing, Softbank was a client of Cybereason, which Ken Miyauchi, president of SoftBank, noted when making the following statement after Softbank's initial investment in Cybereason:

SoftBank works to obtain cutting edge technology and outstanding business models to lead the Information Revolution. Our deployment of the Cybereason platform internally gave us firsthand knowledge of the value it provides, and led to our decision to invest. I'm confident Cybereason and SoftBank's new product offering will bring a new level of security to Japanese organizations."

SoftBank — one of Japan's largest telecommunications companies — not only began to deploy Cybereason internally but directly partnered with it after investing, much like Lockheed Martin had done around the same time. This partnership resulted in SoftBank and Cybereason creating a joint venture in Japan and Cybereason creating partnerships with other tech companies acquired by SoftBank, including the U.K.'s Arm, which specializes in making chips and management platforms for Internet of Things (IoT) devices.

SoftBank's interest in Cybereason is significant, particularly in light of Cybereason's interest in the 2020 U.S. election, given that SoftBank has significant ties to key allies of President Trump and even the president himself.

Indeed, SoftBank's Masayoshi Son was among the first wave of international business leaders who sought to woo then-president-elect Trump soon after the 2016 election. Son first visited Trump Tower in December 2016 and announced, with Trump by his side in the building's lobby, that SoftBank would invest $50 billion in the U.S. and create 50,000 jobs. Trump subsequently claimed on Twitter that Son had only decided to make this investment because Trump had won the election.

Son told reporters at the time that the investment would come from a $100 billion fund that would be created in partnership with Saudi Arabia's sovereign wealth fund as well as other investors. "I just came to celebrate his new job. I said, 'This is great. The US will become great again,'" Son said, according to reports.

Then, in March of 2017, Son sent top SoftBank executives to meet with senior members of Trump's economic team and, according to the *New York Times*, "the SoftBank executives said that because of a lack of advanced digital investments, the competitiveness of the United States economy was at risk. And the executives made the case, quite strongly, that Mr. Son was committed to playing a major role in addressing this issue through a spate of job-creating investments." Many of SoftBank's investments and acquisitions in the U.S. since then have focused mainly on artificial intelligence and technology with military applications, such as "killer robot" firm Boston Dynamics, suggesting Son's interest lies more in dominating futuristic military-industrial technologies than creating jobs for the average American.

After their initial meeting, Trump and Son met again a year later in June 2018, with Trump stating that "His [Son's] $50 billion turned out to be $72 billion so far, he's not finished yet." Several media reports have claimed that Son's moves since Trump's election have sought to "curry favor" with the President.

Through the creation of this fund alongside the Saudis, SoftBank has since become increasingly intertwined with Saudi Crown Prince Muhammad bin Salman (MBS), a key ally of President Trump in the Middle East known for his authoritarian crackdowns on Saudi elites and dissidents alike. The ties between Saudi Arabia and SoftBank became ever tighter when MBS took the reins in the oil kingdom and after SoftBank announced the launch of the Vision Fund in 2016. SoftBank's Vision Fund is a vehicle for investing in hi-tech companies and start-ups and its largest shareholder is the Public Investment Fund of Saudi Arabia. Notably, Son decided to launch the Vision Fund in Riyadh during President Trump's first official visit to the Gulf Kingdom.

In addition, the Mubadala Investment Company, a government fund of the United Arab Emirates (UAE), gave $15 billion to the Vision Fund. UAE leadership also share close ties to the Trump administration and MBS in Saudi Arabia.

As a consequence, SoftBank's Vision Fund is majority funded by two Middle Eastern authoritarian governments with close ties to the U.S. government, specifically the Trump administration. In addition, both countries have enjoyed the rapid growth and normalization of ties with the state of Israel in recent years, particularly following the rise of current Saudi Crown Prince Muhammad bin Salman and Jared Kushner's rise to prominence in his father-in-law's administration. Other investments in the Vision Fund have come from Apple, Qualcomm and Oracle's Larry Ellison, all tech companies with strong ties to Israel's government.

The Saudi and Emirati governments' links to the Vision Fund are so obvious that even mainstream outlets like *the New York Times* have described them as a "front for Saudi Arabia and perhaps other countries in the Middle East."

SoftBank also enjoys close ties to Jared Kushner, with Fortress Investment Group lending $57 million to Kushner Companies in October 2017 while it was under contract to be acquired by SoftBank.
As *Barron's* noted at the time:

When SoftBank Group bought Fortress Investment Group last year, the Japanese company was buying access to a corps of seasoned investors. What SoftBank also got is a financial tie to the family of President Donald Trump's senior advisor and son-in-law, Jared Kushner."

According to *The Real Deal*, Kushner Companies obtained the financing from Fortress only after its attempts to obtain funding through the EB-5 visa programfor a specific real estate venture were abandoned after the U.S. Attorney and the Securities and Exchange Commission began to investigate how Kushner Companies used the EB-5 investor visa program. A key factor in the opening of that investigation was Kushner Companies' representatives touting Jared Kushner's position at the White House when talking to prospective investors and lenders.

SoftBank also recently came to the aid of a friend of Jared Kushner, former CEO of WeWork Adam Neumann. Neumann made shocking claims about his ties to both Kushner and Saudi Arabia's MBS, even asserting that he had worked with both in creating Kushner's long-awaited and controversial Middle East "peace plan" and claimed that he, Kushner and MBS would together "save the world."
Neumann previously called Kushner his "mentor." MBS has also discussed on several occasions his close ties with Kushner and U.S. media reports have noted the frequent correspondence between the two "princelings."

Notably, SoftBank invested in Neumann's WeWork using money from the Saudi-dominated Vision Fund and later went on to essentially bail the company out after its IPO collapse and Neumann was pushed out. SoftBank's founder, Masayoshi Son, had an odd yet very close relationship with Neumann, perhaps explaining why Neumann was allowed to walk with $1.7 billion after bringing WeWork to the brink of collapse. Notably, nearly half of SoftBank's approximately $47 billion investments in the U.S. economy since Trump's election, went to acquiring and then bailing out WeWork. It is unlikely that such a disastrous investment resulted in the level of job creation that Son had promised Trump in 2016.

Given that it is Cybereason's top investor and shareholder by a large margin, SoftBank's ties to the Trump administration and key allies of that administration are significant in light of Cybereason's odd interest in 2020 U.S. election scenarios that end with the cancellation of this year's upcoming presidential election. It goes without saying that the cancellation of the election would mean a continuation of the Trump administration until new elections would take place.

Furthermore, with Cybereason's close and enduring ties to Israeli military intelligence now well-documented, it is worth asking if Israeli military intelligence would consider intervening in 2020 if the still-to-be-decided Democratic contender was strongly opposed to Israeli government policy, particularly Israel's military occupation of Palestine. This is especially worth considering given revelations that sexual blackmailer and pedophile Jeffrey Epstein, who targeted prominent U.S. politicians, mostly Democrats, was in the employ of Israeli military intelligence.

Notably, Cybereason's doomsday election scenarios involved the weaponization of deep fakes, self-driving cars and the hacking Internet of Things devices, with all of those technologies being pioneered and perfected — not by Russia, China or Iran — but by companies directly tied to Israeli intelligence, much like Cybereason itself. These companies, their technology and Cybereason's own work creating the narrative that U.S. rival states seek to undermine the U.S. election in this way, will all be discussed in the conclusion of *MintPress'* series on Cybereason and its outsized interest in the U.S. democratic process.

cybersecurity israel Saudi simulations spies u.s. military

Author

Whitney Webb

Whitney Webb has been a professional writer, researcher and journalist since 2016. She has written for several websites and, from 2017 to 2020, was a staff writer and senior investigative reporter for Mint Press News. She currently writes for The Last American Vagabond.